Title	ゲーム理論と暗号プロトコル (符号と暗号の代数的数理)
Author(s)	鈴木, 幸太郎
Citation	数理解析研究所講究録 (2005), 1420: 138-141
Issue Date	2005-04
URL	http://hdl.handle.net/2433/47170
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録 1420 巻 2005 年 138-141

ゲーム理論と暗号プロトコル

鈴木幸太郎
NTT 情報流通プラットフォーム研究所
suzuki.koutarou@lab.ntt.co.jp

Abstract

本稿では、近年盛んになっているゲーム理論と計算機科学を融合させる研究、特にゲーム理論と暗号プロトコルを融合させる研究について概説し、例として、Vickrey オークションとそれを安全に実現する暗号プロトコルについて説明する。

1 Introduction

近年のインターネットの急速な発展を背景として、ゲーム理論と計算機科学を融合させる研究が盛んになってきている。インターネットは多数の計算機がネットワークを介して繋がれたものであり、計算機科学の扱う対象である。しかしその一方で、インターネットは多数の独立した経済主体により運営されるネットワークが繋がれたものであり、ゲーム理論の扱う対象でもある。このような二面性を持つインターネットを扱うためには、ゲーム理論と計算機科学を組み合わせた手法が必要となってくる [Pap01]。

特に、ゲーム理論をインターネットでのアルゴリズム設計に生かすという観点からは、ゲーム理論の一分野であるメカニズムデザインという手法が重要である。これは、報酬制度（＝メカニズム）をうまく設計して、参加者が正直に自分の秘密情報を申告することで利得が最大化されるようにし、利得を最大化しようとする利己的な参加者に自主的に正直に申告させるという手法である。インターネットにおいては、分散サーバに計算能力を正直に申告させタスクを最適に割り当てる、電子商取引において価格を正直に申告させ財を最適に割り当てる、など数多くのメカニズムデザインの適用先が考えられる。

このようなメカニズムをインターネット上で実行するには、メカニズムの結果をネットワークを介して分散計算する必要がある。そこで、メカニズムを計算する計算量を解析し、メカニズムを効率よく計算できる（分散）アルゴリズムを設計することを目的とする、アルゴリズミックメカニズムデザインという考え方が提唱されている [NR99, Nis99]。その一例として、ルーティングにメカニズムデザインを適用して、最適なルーティングを実現する方法が提案されている [FPSS02]。

しかし、メカニズムの参加者がメカニズムの結果を分散計算する場合、計算結果を改変しようという誘因がはたらく。また、申告した秘密情報を公開したくないという要求もある。そこで、暗号技術により入力を秘匿したまま計算結果の正しさを検証できる暗号プロトコルを用いて、メカニズムの結果を分散計算する方法が提案されている。特に、オークションにおけるメカニズムデザインに関しては、Vickrey オークション [Vic61] の入札結果を入札価格を秘匿したまま不正なく計算する暗号プロトコル [AS02] など、多数の研究がある。

このほかにも、暗号プロトコルを用いて公平な乱数を共有することにより相関均衡を実現する [DHR00]、暗号プロトコルに対する能動攻撃の誘因をなくすことに

より能動攻撃を抑制する [YS04]、秘密分散プロトコルのゲーム理論的解析 [HT04]、などのゲーム理論と暗号プロトコルに関する研究がなされている。

以下では、メカニズムデザインと暗号プロトコルがいかに組み合わされるかを示す例として、Vickrey オークションとそれを安全に実行する暗号プロトコルについて説明する。2 節で Vickrey オークション [Vic61] について説明し、3 節で Vickrey オークションを安全に実行する暗号プロトコル [AS02] を説明し、4 節でまとめる。

2 Vickrey Auction

本節では、メカニズムデザインの最も基本的で本質的な例である Vickrey オークション [Vic61] について説明する。以下のような状況を考える。

- 開札者が 1 つの財を入札にかけ、n 人の入札者 $i = 1, ..., n$ がそれを落札する。
- 入札者 i は、入札にかけられる財に対して真の価値 v_i（出せるぎりぎりの額）をもっていて、他者はその額を知らない（私的価値）。
- 入札者 i が p を支払い財を落札したとき、入札者 i は効用 $v_i - p$ を得（準線形効用）、開札者は効用 p を得る。

Vickrey オークション（第二価格入札）とは以下のような封印入札である。

- 入札：入札者 i は、入札価格 b_i を封印して入札する。
- 開札：すべての入札者が入札を終えた後封印を開き、最も高い入札価格をつけた入札者 i_{1st} が二番目に高い入札価格 b_{2nd} を支払い落札する。

この一見奇妙にみえる Vickrey オークションは、以下の望ましい性質を満たしている。

- 誘因両立性：真の価値を入札する（つまり $b_i := v_i$ とする）ことが、支配戦略（つまり他の入札者のすべての戦略に対しての最適戦略）となる。（つまり入札者は自主的に真の価値を入札する。）
- Pareto 効率性：支配戦略均衡（つまりすべての入札者が支配戦略を取った状態）において、すべての入札者と開札者の効用の和は最大化される。（つまり最も真の価値が高い入札者が財を落札し財の最適割り当てが実現される。）
- 個人合理性：支配戦略均衡において、すべての入札者と開札者の効用は負にならない。（つまり入札者および開札者は入札に参加することで損をしないので参加することが合理的。）

Theorem 1 *Vickrey* オークションは誘因両立性、*Pareto* 効率性、個人合理性を満たす。

Proof: 入札者 i が真の価値 v_i を入札して落札できる場合、入札価格を真の価値 v_i 以外に変えても、落札できる場合は効用は $v_i - b_{2nd} \geq 0$ で変化せず、落札できない場合は効用は 0 となり増加しないので、真の価値を入札することが支配戦略である。

入札者 i が真の価値 v_i を入札して落札できない場合、入札価格を真の価値 v_i 以外に変えても、落札できない場合は効用は 0 で変化せず、落札できる場合は効用は $v_i - b_{2nd} \leq 0$ となり増加しないので、真の価値を入札することが支配戦略である。

すべての入札者と開札者の効用の和は落札者 i の真の価値 v_i となるが、すべての入札者が真の価値を入札する支配戦略均衡では真の価値 v_i が最大の i が落札するため効用の和は最大化される。

すべての入札者が真の価値を入札する支配戦略均衡では、落札者 i は真の価値 v_i を入札して落札しているので $v_i = b_i \geq b_{2nd}$ であり効用 $v_i - p = v_i - b_{2nd}$ は負にならない。また、開札者の効用 $p = b_{2nd}$ は負にならない。 ◇

このようにVickreyオークションにおいては、二番目に高い入札価格を支払額とすることにより、入札者に秘密の真の価値を正直に申告させることができ、それによって財の最適な割り当てを実現することができる。このように参加者に正直に申告させることは、他の方法では実現することができないメカニズムデザインならではの効果である。

3 Secure Vickrey Auction Protocol

本節では、Vickreyオークションを安全に実行する暗号プロトコル[AS02]について説明する。前述のようにVickreyオークションは優れた特徴を持っているが、Vickreyオークションを入札者たちが分散計算する場合、以下のような問題がある。

- オークションの計算結果を改変し利益を得ようとする。
- 入札した真の価値は重要な秘密情報であり公開したくない。

そこで、入札価格を秘匿しつつオークションの計算結果の正しさを検証できる、Vickreyオークションを実現する以下のような暗号プロトコルが提案されている[AS02]。

- 準備：Eを準同型性$E(a)E(b)=E(ab)$を満たす安全な（IND-CPAな）公開鍵暗号（例えばElGamal暗号）とする（暗号化をE、復号化をDと書く）。分散復号サーバは、Eの鍵を分散生成し公開鍵を公開し、$z\neq 1$を公開する。開札者は、入札価格表$\{1,2,\cdots,p\}$を公開する。
- 入札：入札者iは、入札価格b_iを決め、それを暗号化したもの$(c_{1,i},...,c_{p,i})$

$$c_{j,i}=\begin{cases} E(z) & \text{if } j\leq b_i \\ E(1) & \text{if } b_i<j \end{cases}$$

と正しく作っていることの非対話ゼロ知識証明を公開して、入札を行なう。

- 開札:すべての入札者が入札を終えた後、開札者は、$c_j=c_{j,1}\cdots c_{j,n}$ $(1\leq j\leq p)$を計算し公開する。ここで、準同型性$E(a)E(b)=E(ab)$により、

$$c_j=E(z^{n(j)}),\ n(j)=\#\{i\mid j\leq b_i\}$$

となっていることに注意する。

つぎに、分散復号サーバによる（証明つきの）分散復号とmix and match[JJ00]の手法により、$D(c_j)\in\{1,z,z^2\}$かどうか判定することができるので、$\lceil\log p\rceil$回この判定を繰り返すことにより、二番目に高い入札価格$b_{2\text{nd}}$ s.t. $n(b_{2\text{nd}})\geq 2$ and $n(b_{2\text{nd}}+1)\leq 1$を求めることができる。

つぎに、$c_{b_{2\text{nd}}+1,i}$ $(1\leq i\leq n)$を（証明つきで）分散復号することにより、落札者$i_{1\text{st}}$ s.t. $D(c_{b_{win}+1,i_{1\text{st}}})=z$を求めることができる。

最後に、落札者$i_{1\text{st}}$と支払価格$b_{2\text{nd}}$を入札結果として公開する。

公開鍵暗号Eの安全性により、入札価格の秘匿が保証される。また、非対話ゼロ知識証明がついているため、計算結果の正しさを検証することができる。また、必要な通信回数は$O(n+\log p)$であり、秘匿回路計算[BOGW88, CCD88]を用いた場合の必要な通信回数$O(n^2\times n\log p)$と比較して、効率的である。

4 Conclusions

ゲーム理論と暗号プロトコルを融合させる研究について概説し、例として、Vickrey オークションとそれを安全に実現する暗号プロトコルについて説明した。メカニズムデザインとそのメカニズムを実行する暗号プロトコルにより、参加者に正直に申告させられるというメカニズムデザインならではの効果と、申告した秘密情報を秘匿しつつメカニズムの計算の正しさを検証できるという暗号プロトコルならではの効果とを、相補的に組み合わせることができた。

References

[AS02] Masayuki Abe and Koutarou Suzuki. M+1-st price auction using homomorphic encryption. In *Public Key Cryptography 2002*, pages 115–124, 2002.

[BOGW88] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In *STOC 1988*, pages 1–10, 1988.

[CCD88] David Chaum, Claude Crepeau, and Ivan Damgard. Multiparty unconditionally secure protocols (extended abstract). In *STOC 1988*, pages 11–19, 1988.

[DHR00] Yevgeniy Dodis, Shai Halevi, and Tal Rabin. A cryptographic solution to a game theoretic problem. In *CRYPTO 2000*, pages 112–130, 2000.

[FPSS02] Joan Feigenbaum, Christos H. Papadimitriou, Rahul Sami, and Scott Shenker. A bgp-based mechanism for lowest-cost routing. In *PODC 2002*, pages 173–182, 2002.

[HT04] Joseph Y. Halpern and Vanessa Teague. Rational secret sharing and multiparty computation: extended abstract. In *STOC 2004*, pages 623–632, 2004.

[JJ00] Markus Jakobsson and Ari Juels. Mix and match: Secure function evaluation via ciphertexts. In *ASIACRYPT 2000*, pages 162–177, 2000.

[Nis99] Noam Nisan. Algorithms for selfish agents. In *STACS 1999*, pages 1–15, 1999.

[NR99] Noam Nisan and Amir Ronen. Algorithmic mechanism design (extended abstract). In *STOC 1999*, pages 129–140, 1999.

[Pap01] Christos H. Papadimitriou. Algorithms, games, and the internet. In *STOC 2001*, pages 749–753, 2001.

[Vic61] William Vickrey. Counterspeculation, auctions, and competitive sealed tenders. In *Journal of Finance*, pages 8–37, 1961.

[YS04] Makoto Yokoo and Koutarou Suzuki. Secure generalized vickrey auction without third-party servers. In *Financial Cryptography 2004*, pages 132–146, 2004.